

# *Mathematical Journal of Okayama University*

---

*Volume 15, Issue 1*

1971

*Article 12*

DECEMBER 1971

---

## On cyclic extensions of commutative rings

Takasi Nagahara<sup>\*</sup>

Atsushi Nakajima<sup>†</sup>

<sup>\*</sup>Okayama University

<sup>†</sup>Okayama University

Copyright ©1971 by the authors. *Mathematical Journal of Okayama University* is produced by The Berkeley Electronic Press (bepress). <http://escholarship.lib.okayama-u.ac.jp/mjou>

## ON CYCLIC EXTENSIONS OF COMMUTATIVE RINGS

Dedicated to Professor Takeshi Inagaki on his 60th birthday

TAKASI NAGAHARA and ATSUSHI NAKAJIMA

In [3], K. Kishimoto presented a theory of abelian extensions of rings which contains a theory of cyclic extensions of commutative rings without proper idempotents. In this paper, we give a sharpening of Kishimoto's theory for commutative rings, and we also generalize some classical theorems in the theory of abelian extensions of fields to commutative rings. In §1, we shall give a theory of cyclic extensions of commutative rings. §2 is devoted to studying abelian extensions as an application of the theory of §1.

In all that follows  $B$  will mean a commutative algebra over the prime field  $GF(p)$  ( $p \neq 0$ ), and all ring extensions of  $B$  will be assumed to be commutative and have identities coinciding with the identity of  $B$ . As to other terminologies used in this paper, we follow [1] and [2].

The following lemma is useful in our paper

**Lemma 0.** *Let  $\mathfrak{G}$  be a finite cyclic group of automorphisms in an arbitrary ring  $A$  which is generated by  $\sigma$ . If there exist elements  $a$  and  $b$  in  $A$  such that  $t_{\mathfrak{G}}(a) (= \sum_{\tau \in \mathfrak{G}} \tau(a)) = 1$  and  $t_{\mathfrak{G}}(b) = 0$  then there exists an element  $c$  in  $A$  such that  $\sigma(c) = c + b$ .*

In fact, if we correspond  $\sigma \rightarrow b$ ,  $\sigma^2 \rightarrow b + \sigma(b)$ ,  $\dots$ ,  $\sigma^n \rightarrow b + \sigma(b) + \dots + \sigma^{n-1}(b)$  where  $n$  is the order of  $\mathfrak{G}$ , then by [5, §10, p. 65], we have the requested result.

**1. Cyclic extensions of commutative rings.** A ring extension  $A$  of  $B$  will be called a cyclic  $p^n$ -extension of  $B$  (with a Galois group  $(\sigma)$ ) if  $A$  is a Galois extension of  $B$  with a cyclic Galois group  $(\sigma)$  of order  $p^n$ .

**Lemma 1.1.** *Let  $f(X) = X^n - X - b_0 \in B[X]$ . Then  $f(X)$  is separable. If there is a ring extension  $A$  of  $B$  which contains an element  $a$  such that  $f(a) = 0$  then  $f(X) = (X - a)(X - (a + 1)) \cdots (X - (a + p - 1))$ ; and if, in addition, there exists a  $B$ -algebra automorphism  $\sigma$  such that  $\sigma(a) = a + 1$*

then there exists an isomorphism

$$(i) \quad B[X]/(f(X)) \rightarrow B[a]$$

such that  $g(X) \mapsto g(a)$ .

*Proof.* The first assertion is the result of [4, Cor. 4]. The second assertion is proved by making use of the same method as in the proof of [4, Lemma].

**Theorem 1.1.** Let  $f(X) = X^p - X - b_0 \in B[X]$ . Then  $B[X]/(f(X))$  is a cyclic  $p$ -extension of  $B$  with a Galois group generated by an automorphism

$$(ii) \quad B[X]/(f(X)) \rightarrow B[X]/(f(X))$$

such that  $X \mapsto X+1$ .

*Proof.* The map  $\sum_i b_i X^i \mapsto \sum_i b_i (X+1)^i$  defines an automorphism of  $B[X]$  sending  $f(X)$  into  $f(X+1) = f(X)$ . Hence this induces an automorphism  $\sigma$  of  $B[X]/(f(X))$ . Clearly the cyclic group  $\langle \sigma \rangle$  generated by  $\sigma$  is of order  $p$ . Set  $x = X \mapsto (f(X))$  and let  $B'$  be the fixring of  $\langle \sigma \rangle$  in  $B[x]$ . Then, for  $c' \in B'$ , we may write  $c' = \sum_{i=0}^{p-1} c_i x^i$  where the  $c_i$  are elements of  $B$ . Hence we have  $\sum_{i=0}^{p-1} c_i (\sigma^j(x))^i \mapsto (c_0 - c') (\sigma^j(x))^0 = 0$  ( $0 \leq j < p$ ). The determinant of the matrix  $\|(\sigma^j(x))^i\|$  ( $0 \leq i, j < p$ ) is  $\pm \prod_{j < k} (\sigma^j(x) - \sigma^k(x))$  which is invertible in  $B[x]$ . This implies  $c_0 - c' = 0$ , that is,  $c_0 = c'$ . Thus we obtain  $B' = B$ . Therefore, by [4, Lemma],  $B[x]$  is a Galois extension of  $B$  with a Galois group  $\langle \sigma \rangle$ .

The following corollary is a direct consequence of Lemma 1.1 and Th. 1.1.

**Corollary 1.1.** Let  $A$  be a ring extension of  $B$ , and  $\sigma$  a  $B$ -algebra automorphism of  $A$ . If there exists an element  $a$  of  $A$  such that  $a^p - a \in B$  and  $\sigma(a) = a+1$ . Then there exist isomorphisms

$$\begin{array}{ccc} & (i) & \\ B[X]/(f(X)) & \longrightarrow & B[a] \\ (ii) \downarrow & & \downarrow \sigma|B[a] \\ & (i) & \\ B[X]/(f(X)) & \longrightarrow & B[a] \end{array}$$

where  $f(X) = X^p - X - (a^p - a)$  and  $\sigma|B[a]$  is the restriction of  $\sigma$  to  $B[a]$ ;

hence  $B[a]$  is a cyclic  $p$ -extension of  $B$  with a Galois group  $(\sigma|B[a])$ .

**Theorem 1.2.** *Let  $A$  be a cyclic  $p$ -extension of  $B$  with a Galois group  $(\sigma)$ . Then there exists an element  $a$  in  $A$  such that  $\sigma(a)=a+1$ . In this case, there holds that  $a^p-a \in B$  and  $B[a]=A$ ; and there exists an isomorphism*

$$(i) \quad B[X]/(f(X)) \rightarrow A$$

where  $f(X)=X^p-X-(a^p-a)$ .

*Proof.* By Lemma 0 and [1, Lemma 1.6], there exists an element  $a$  in  $A$  such that  $\sigma(a)=a+1$ . Then  $a^p-a \in B$ . Hence by Cor. 1.1,  $B[a]$  is a cyclic  $p$ -extension of  $B$  with a Galois group  $(\sigma|B[a])$ ; whence there exist elements  $x_1, \dots, x_n; y_1, \dots, y_n$  of  $B[a]$  such that  $\sum_{i=1}^n x_i \sigma^{j-1}(y_i) = \delta_{1,j}$  for  $1 \leq j \leq p$ . Then for every  $u \in A$ , we have  $u = \sum_{i=1}^n x_i t_{(\sigma)}(uy_i) \in B[a]$ . This implies  $B[a]=A$ .

As a corollary to Th. 1.2, we have the following

**Corollary 1.2.** *Let  $A$  and  $A'$  be cyclic  $p$ -extensions of  $B$  with Galois groups  $(\sigma)$  and  $(\sigma')$  respectively which contain elements  $a$  and  $a'$  respectively such that  $\sigma(a)=a+1$ ,  $\sigma'(a')=a'+1$  and  $a^p-a=a'^p-a'$ . Then  $A=B[a] \cong A'=B[a'](a \mapsto a')$  as  $B$ -algebras.*

**Theorem 1.3.** *Let  $A$  be a cyclic  $p^e$ -extension of  $B$  with a Galois group  $(\sigma)$ . Then there exist elements  $a, a_0$  in  $A$  such that*

$$t_{(\sigma)}(a)=1, \text{ and } \sigma(a_0)-a_0=a^p-a.$$

*In this case,  $A[X]/(X^p-X-a_0)$  is a cyclic  $p^{e+1}$ -extension of  $B$  with a Galois group generated by an automorphism*

$$(iii) \quad A[X]/(X^p-X-a_0) \rightarrow A[X]/(X^p-X-a_0)$$

*such that  $\sum_i c_i X^i + (X^p-X-a_0) \mapsto \sum_i \sigma(c_i)(X+a)^i + (X^p-X-a_0)$ , which is an extension of  $\sigma$ .*

*Proof.* The first assertion is a direct consequence of [1, Lemma 1.6] and Lemma 0. It will be easily seen that the map  $\sum_i c_i X^i \mapsto \sum_i \sigma(c_i)(X+a)^i$  defines an automorphism of  $A[X]$  sending  $X^p-X-a_0$  into  $(X+a)^p-(X+a)-a_0=X^p-X-a_0$ . Hence this induces an automorphism

$\sigma_0$  of  $A[X]/(X^p - X - a_0)$ . We set  $A[x] = A[X]/(X^p - X - a_0)$  where  $x = X + (X^p - X - a_0)$ . Then  $A \subset A[x]$  is a cyclic  $p^e$ -extension of  $B$  with a Galois group  $(\sigma_0 | A)$ . Since  $\sigma_0^{p^e} | A$  is an identity and  $\sigma_0^{p^e}(x) = x + t_{(\sigma_0)}(a) = x + 1$ , it follows from Cor. 1.1 that  $A[x]$  is a cyclic  $p$ -extension of  $A$  with a Galois group  $(\sigma_0^{p^e})$ . Hence there exist elements  $u_1, \dots, u_m; v_1, \dots, v_m$  of  $A$  and elements  $x_1, \dots, x_n; y_1, \dots, y_n$  of  $A[x]$  such that  $\sum_i u_i \rho(v_i) = \delta_{1,\rho}$  for  $\rho \in (\sigma_0 | A)$  and  $\sum_i x_i \gamma(y_i) = \delta_{1,\gamma}$  for  $\gamma \in (\sigma_0^{p^e})$ . Then  $\sum_{i,j} x_i u_i \pi(v_i y_j) = \delta_{1,\pi}$  for  $\pi \in (\sigma_0)$ . Therefore  $A[x]$  is a cyclic  $p^{e+1}$ -extension of  $B$  with a Galois group  $(\sigma_0)$ .

**Theorem 1.4.** *Let  $A_*$  be a cyclic  $p^{e+1}$ -extension of  $B$  with a Galois group  $(\sigma_*)$ . Let  $A$  be the fixing of  $(\sigma_*^{p^e})$  in  $A_*$ . Then  $A$  is a cyclic  $p^e$ -extension of  $B$  with a Galois group  $(\sigma)$  generated by  $\sigma = \sigma_* | A$  and there exist elements  $a, a_0$  in  $A$  and an  $A$ -algebra isomorphism (i') such that*

$$t_{(\sigma)}(a) = 1, \quad \sigma(a_0) - a_0 = a^p - a,$$

and the following diagram

$$\begin{array}{ccc} & & \text{(i')} \\ & & A[X]/(X^p - X - a_0) \longrightarrow A_* \\ \text{(iii)} \downarrow & & \downarrow \sigma_* \\ & & \text{(i')} \\ A[X]/(X^p - X - a_0) & \longrightarrow & A_* \end{array}$$

is commutative where (i') is defined as for  $B[X]/(f(X))$  in Lemma 1.1, and (iii) is given by

$$\sum_i c_i X^i + (X^p - X - a_0) \rightarrow \sum_i \sigma_*(c_i)(X + a)^i + (X^p - X - a_0).$$

*Proof.* It is obvious that  $A$  is a cyclic  $p^e$ -extension of  $B$  with a Galois group  $(\sigma)$  generated by  $\sigma = \sigma_* | A$ . Hence there exists an element  $a$  of  $A$  such that  $t_{(\sigma)}(a) = 1$ . Noting  $t_{(\sigma_*)}(a) = 0$ , there exists an element  $x$  of  $A_*$  such that  $\sigma_*(x) = x + a$ . Then  $\sigma_*^{p^e}(x) = x + t_{(\sigma_*)}(a) = x + 1$ . We set  $a_0 = x^p - x$ . Then  $a_0 \in A$  and  $\sigma_*(a_0) - a_0 = (x + a)^p - (x + a) - a_0 = a^p - a$ . Since  $\sigma_*^{p^e}(x) = x + 1$ , by Th. 1.2, we have an  $A$ -algebra isomorphism

$$\text{(i')} \quad A[X]/(X^p - X - a_0) \rightarrow A[x] = A_*$$

such that  $X + (X^p - X - a_0) \rightarrow x$ . Then the diagram as in the theorem is commutative.

**Theorem 1.5.** *Let  $A$  be a cyclic  $p^e$ -extension of  $B$  with a Galois group  $(\sigma)$ . Then*

(1) *if  $C$  is a  $B$ -algebra with an identity element then  $C \otimes_B A$  is a cyclic  $p^e$ -extension of  $C$  (identifying  $C \otimes 1$ ) with a Galois group  $(1 \otimes \sigma)$ .*

(2) *If  $N$  is a proper ideal of  $B$  then  $AN \cap B = N$  and  $A/AN (\cong B/N \otimes_B A)$  is a cyclic  $p^e$ -extension of  $B/N$  (with a Galois group  $(1 \otimes \sigma)$ ).*

(3) *If  $S$  is a multiplicatively closed subset of  $B$  containing 1 but not containing 0 then the quotient ring  $A[S^{-1}] (\cong B[S^{-1}] \otimes_B A)$  is a cyclic  $p^e$ -extension of  $B[S^{-1}]$  (with a Galois group  $(1 \otimes \sigma)$ ).*

*Proof.* (1) Since  $B$  is a direct summand of a  $B$ -module  $A$ , we have  $C \cong C \otimes B \subset C \otimes_B A$ . Clearly  $1 \otimes \sigma$  is a  $C \otimes B$ -algebra automorphism of  $C \otimes_B A$  such that  $(1 \otimes \sigma)^{p^e}$  is an identity. Let  $B_i$  be the fixring of  $(\sigma^{p^i})$  in  $A$ . Then  $B = B_0 \subset B_1 \subset \cdots \subset B_e = A$  and for every  $i < e$ ,  $B_{i+1}$  is a cyclic  $p$ -extension of  $B_i$  with a Galois group  $(\sigma^{p^i}|_{B_{i+1}})$ ; hence by Th. 1.2, there exists an element  $u$  in  $B_{i+1}$  such that  $B_i[u] = B_{i+1}$ ,  $u^p - u \in B_i$ , and  $\sigma^{p^i}(u) = u + 1$ . Then  $(C \otimes B_i)[1 \otimes u] = C \otimes B_{i+1}$ ,  $(1 \otimes u)^p - 1 \otimes u \in C \otimes B_i$ , and  $(1 \otimes \sigma)^{p^i}(1 \otimes u) = 1 \otimes u + 1 \otimes 1$ . Hence by Cor. 1.1,  $C \otimes B_{i+1}$  is a cyclic  $p$ -extension of  $C \otimes B_i$  with a Galois group  $((1 \otimes \sigma)^{p^i}|_{C \otimes B_{i+1}})$ . Therefore  $C \otimes_B A$  is a cyclic  $p^e$ -extension of  $C \otimes B$  with a Galois group  $(1 \otimes \sigma)$ . Thus we obtain (1). As corollaries to (1), we have (2) and (3).

Let  $B$  be an arbitrary ring with an identity.  $f(X) \in B[X]$  will be called irreducible in  $B[X]$  if each proper factor of  $f(X)$  is contained in  $B$ . For an irreducible polynomial, we have the following

**Lemma 1.2.** *Let  $B$  be a ring without proper idempotents, and  $f(X) = X^p - X - b_0 \in B[X]$ . Then,  $f(X)$  is irreducible if and only if  $f(b) \neq 0$  for each  $b \in B$ .*

*Proof.* Let  $f(b) \neq 0$  for each  $b \in B$ . Set  $f(X) = g(X)h(X)$  where  $g(X)$  is a monic polynomial in  $B[X]$  of positive degree. Then by Lemma 1.1,  $f(X)$  is separable and so  $g(X)$  is separable. Hence by [2, Th. 2.2], there is a Galois extension  $A$  of  $B$  without proper idempotents which contains an element  $a$  such that  $f(a) = 0$ . From  $f(a) = 0$ , we have  $f(X) = (X - a)(X - (a + 1)) \cdots (X - (a + p - 1))$ . Since  $a \notin B$ , there exists a  $B$ -algebra automorphism  $\sigma$  of  $A$  such that  $\sigma(a) \neq a$ . Then, by [2, Lemma 2.1], we have  $\sigma(a) = a + m$ ,  $0 < m < p$ . On the other hand, let  $C$  be a splitting ring of

$g(X)$  over  $A$  without proper idempotents. Then there exists an element  $c \in C$  with  $g(c) = 0$ . Since  $f(c) = 0$ , we have  $c = a + i = \sigma^i(a)$  for some  $i$  ( $0 \leq i < p$ ) and  $k$ . Therefore we obtain  $\deg g(X) \geq p$ ; this implies  $g(X) = f(X)$ . Thus  $f(X)$  is irreducible. The converse is obvious.

**Theorem 1.6.** *Let  $B$  be a ring without proper idempotents, and  $f(X) = X^p - X - b_0 \in B[X]$ . Then,  $B[X]/(f(X))$  has no proper idempotents if and only if  $f(b) \neq 0$  for each  $b \in B$ .*

*Proof.* By Lemma 1.1,  $f(X)$  is separable. Hence,  $B[X]/(f(X))$  has no proper idempotents if and only if  $f(X)$  is irreducible. By Lemma 1.2, this is equivalent to that  $f(b) \neq 0$  for each  $b \in B$ .

As a direct consequence of Th. 1.1 and Th. 1.6, we have the following theorem which contains the result of [3, Th. 3.1].

**Theorem 1.7.** *Let  $B$  be a ring without proper idempotents. Then, there is a cyclic  $p$ -extension of  $B$  without proper idempotents if and only if there is an element  $b_0$  of  $B$  such that  $b^p - b - b_0 \neq 0$  for each  $b \in B$ .*

**Corollary 1.3.** *Let  $A$  be a cyclic  $p$ -extension of  $B$  without proper idempotents. If  $a$  is an element of  $A$  such that  $a^p - a \in B$  and  $a \notin B$  then  $A = B[a] \cong B[X]/(X^p - X - b_0)$  where  $b_0 = a^p - a$ .*

*Proof.* Let  $(\sigma)$  be the Galois group of the cyclic  $p$ -extension  $A$  of  $B$ , and  $a$  an element of  $A$  such that  $a^p - a = b_0 \in B$  and  $a \notin B$ . Then  $\sigma(a) \neq a$ . Since  $f(X) = X^p - X - b_0$  is separable and  $f(\sigma(a)) = 0$ , it follows from [2, Lemma 2.1] that  $\sigma(a) \in \{a, a+1, \dots, a+p-1\}$ ; hence  $\sigma(a) = a+m$ ,  $0 < m < p$ . Hence  $\sigma^i(a) = a+i$  for some  $i$ . Then by Th. 1.2, we have  $B[X]/(f(X)) \cong B[a] = A$ .

From Cor. 1.3, we have the following

**Corollary 1.4.** *Let  $A_1, A_2$  be cyclic  $p$ -extensions of  $B$  without proper idempotents. Then,  $A_1 \cong A_2$  as  $B$ -algebras if and only if there exist elements  $a_1 \in A_1$  and  $a_2 \in A_2$  such that  $a_1^p - a_1 = a_2^p - a_2 \in B$  and  $a_1 \notin B$ .*

**Lemma 1.3.** *Let  $A$  be a cyclic  $p$ -extension of  $B$  with a Galois group  $(\sigma)$  which has no proper idempotents. If  $a, a_0$  are elements in  $A$  such that  $\sigma(a_0) - a_0 = a^p - a$  and  $t_{(\sigma)}(a) = 1$  then  $A[X]/(X^p - X - a_0)$  has no proper idempotents.*

*Proof.* Suppose that  $t^n - t - a_0 = 0$  for some  $t \in A$ . Then  $a^p - a = \sigma(a_0) - a_0 = (\sigma(t) - t)^p - (\sigma(t) - t)$ . Hence  $(\sigma(t) - t - a)^p - (\sigma(t) - t - a) = 0$ . Since the polynomial  $X^p - X$  is separable, it follows that  $\sigma(t) - t - a$  is an element of  $GF(p)$ ; then  $t_{(\omega)}(\sigma(t) - t - a) = 0$ . On the other hand, we have  $t_{(\omega)}(\sigma(t) - t - a) = t_{(\omega)}(-a) = -1$ . This is a contradiction. Hence by Th. 1.6, we obtain our assertion.

The result of the following lemma is well known.

**Lemma 1.4.** *Let  $A$  be a Galois extension of  $B$ . Let  $M$  be a maximal ideal of  $B$ . Then*

- (1) *there exist maximal ideals  $M_1, \dots, M_n$  of  $A$  such that  $M_1 \cap \dots \cap M_n = AM$ .*
- (2) *If  $A$  is a local ring with a maximal ideal  $M_*$  then  $B$  is a local ring with a maximal ideal  $B \cap M_*$  and  $M_* = A(B \cap M_*)$ .*
- (3) *When  $B$  is a local ring with a maximal ideal  $M$ ,  $A$  is a local ring if and only if  $AM$  is a maximal ideal of  $A$ .*
- (4)  *$B$  is a semi-local ring if and only if so is  $A$ .*

**Theorem 1.8.** *Let  $A$  be a cyclic  $p^e$ -extension of  $B$  with a Galois group  $(\sigma)$ , and  $B_1$  the fixring of  $(\sigma^v)$  in  $A$ . Then*

- (1)  *$A$  has no proper idempotents if and only if  $B_1$  has no proper idempotents.*
- (2)  *$A$  is a field if and only if  $B_1$  is a field.*
- (3)  *$A$  is a domain if and only if  $B_1$  is a domain.*
- (4)  *$A$  is a local ring if and only if  $B_1$  is a local ring.*

*Proof.* For  $0 \leq i \leq e$ , let  $B_i$  be the fixring of  $(\sigma^{p^i})$  in  $A$ . Then  $B \subset B_1 \subset B_2 \subset \dots \subset B_e = A$ , and for  $j > i$ ,  $B_j$  is a cyclic  $p^{j-i}$ -extension of  $B_i$  with a Galois group  $(\sigma^{p^i} | B_j)$ . Hence (1) is a direct consequence of Th. 1.4 and Lemma 1.3. (2) follows from (1). (3) Let  $B_1$  be a domain. Let  $Q_1$  be the quotient field of  $B_1$  and  $Q$  the quotient field of  $B$  in  $Q_1$ . Then  $Q[B_1]$  is a finitely generated  $Q$ -module. This implies  $Q_1 = Q[B_1] \cong Q \otimes_B B_1$ . By Th. 1.5,  $Q \otimes_B A$  is a cyclic  $p^e$ -extension of  $Q \otimes_B B$ . Since the canonical homomorphism  $Q \otimes_B B_1 \rightarrow Q \otimes_B A$  is injective, it follows from (2) that  $Q \otimes_B A$  is a field. Noting  $A \cong 1 \otimes A \subset Q \otimes_B A$ ,  $A$  is a domain. (4) If  $A$  is a local ring then, by Lemma 1.4,  $B_1$  is a local ring. To see the converse, let  $B_1$  be a local ring with a maximal ideal  $M_1$ , and set  $M = B \cap M_1$ . Then by Lemma 1.4, we have  $M_1 = B_1 M$ . By Th. 1.5,  $A/AM$  is a cyclic  $p^e$ -extension of



$B/M$ . Since  $B_1/(AM \cap B_1) = B_1/M_1$  is a field, it follows from (2) that  $A/AM$  is a field, that is,  $AM$  is a maximal ideal of  $A$ . Therefore by Lemma 1.4,  $A$  is a local ring.

The following corollary is a direct consequence of Th. 1.5 and Th. 1.8.

**Corollary 1.5.** *Let  $A$  be a cyclic  $p'$ -extension of  $B$  with a Galois group  $(\sigma)$ , and  $B_1$  the fixring of  $(\sigma^p)$  in  $A$ . Let  $C$  be a  $B$ -algebra with an identity element,  $N$  a proper ideal of  $B$ , and  $S$  a multiplicatively closed subset of  $B$  not containing 0. Then*

(1)  $C \otimes_B A$  (resp.  $A/AN$  (resp.  $A[S^{-1}]$ )) has no proper idempotents if and only if  $C \otimes_B B_1$  (resp.  $B_1/B_1N$  (resp.  $B_1[S^{-1}]$ )) contains no proper idempotents.

(2)  $C \otimes_B A$  (resp.  $A/AN$  (resp.  $A[S^{-1}]$ )) is a field if and only if  $C \otimes_B B_1$  (resp.  $B_1/B_1N$  (resp.  $B_1[S^{-1}]$ )) is a field.

(3)  $C \otimes_B A$  (resp.  $A/AN$  (resp.  $A[S^{-1}]$ )) is a domain if and only if  $C \otimes_B B_1$  (resp.  $B_1/B_1N$  (resp.  $B_1[S^{-1}]$ )) is a domain.

(4)  $C \otimes_B A$  (resp.  $A/AN$  (resp.  $A[S^{-1}]$ )) is a local ring if and only if  $C \otimes_B B_1$  (resp.  $B_1/B_1N$  (resp.  $B_1[S^{-1}]$ )) is a local ring.

The following theorem contains the results of [3, Th. 3.2, Th. 5.2]. K. Kishimoto proved (2) and (3) directly. However, the corollary is a direct consequence of Th. 1.3 and Th. 1.8.

**Corollary 1.6.** *Let  $e$  be a positive integer. Then*

(1) *there is a cyclic  $p^e$ -extension of  $B$  which has no proper idempotents if and only if there is a cyclic  $p$ -extension of  $B$  which has no proper idempotents.*

(2) (K. Kishimoto). *There is a cyclic  $p'$ -extension of  $B$  which is a domain if and only if there is a cyclic  $p$ -extension of  $B$  which is a domain.*

(3) (K. Kishimoto). *There is a cyclic  $p^e$ -extension of  $B$  which is a local ring if and only if there is a cyclic  $p$ -extension which is a local ring.*

**2. Abelian extensions of commutative rings.** If  $A$  is an abelian extension of  $B$  with a Galois group  $(\sigma_1) \times (\sigma_2) \times \cdots \times (\sigma_n)$  where for  $i$ ,  $(\sigma_i)$  is of order  $p^{e_i}$  then, it is called to be an abelian  $(p^{e_1}, \dots, p^{e_n})$ -extension of  $B$  (with a Galois group  $(\sigma_1) \times (\sigma_2) \times \cdots \times (\sigma_n)$ ).

The following theorem will be proved easily.

**Theorem 2.1.** *Let  $A_i$  ( $1 \leq i \leq n$ ) be cyclic  $p^{e_i}$ -extension of  $B$  with Galois groups  $(\sigma_i)$ . Then  $A_1 \otimes_B A_2 \otimes \cdots \otimes_B A_n$  is an abelian  $(p^{e_1}, \dots, p^{e_n})$ -extension of  $B$  with a Galois group  $(\sigma_1) \times \cdots \times (\sigma_n)$ .*

The following theorem follows from [1, Th. 2.3] and the fact that every cyclic  $p^e$ -extension of  $B$  is a free  $B$ -module.

**Theorem 2.2.** *Let  $A$  be an abelian  $(p^{e_1}, \dots, p^{e_n})$ -extension with a Galois group  $(\sigma_1) \times \cdots \times (\sigma_n)$ . For each  $i$ , let  $A_i$  be the fixing of  $(\sigma_1) \times \cdots \times (\sigma_{i-1}) \times (\sigma_{i+1}) \times \cdots \times (\sigma_n)$  in  $A$ . Then  $A \cong A_1 \otimes_B A_2 \otimes \cdots \otimes_B A_n$ , and the  $A_i$  are cyclic  $p^{e_i}$ -extensions with Galois groups  $(\sigma_i | A_i)$ .*

Now, we shall prove the following

**Theorem 2.3.** *Let  $A$  be an abelian  $(p^{e_1}, \dots, p^{e_n})$ -extension with a Galois group  $(\sigma_1) \times \cdots \times (\sigma_n)$ . Let  $B_1$  be the fixing of  $(\sigma_1^{p^1}) \times \cdots \times (\sigma_n^{p^1})$  in  $A$ . Then*

- (1)  *$A$  has no proper idempotents if and only if  $B_1$  has no proper idempotents.*
- (2)  *$A$  is a field if and only if  $B_1$  is a field.*
- (3)  *$A$  is a domain if and only if  $B_1$  is a domain.*
- (4)  *$A$  is a local ring if and only if  $B_1$  is a local ring.*

**Proof.** For  $1 \leq i \leq n$  and for  $1 \leq j \leq e_i$ , let  $B_{ij}$  be the fixing of  $(\sigma_1) \times \cdots \times (\sigma_{i-1}) \times (\sigma_i^{p^j}) \times (\sigma_{i+1}) \times \cdots \times (\sigma_n)$  in  $A$ . Then by Th. 2.2, we have  $A \cong B_{1e_1} \otimes \cdots \otimes B_{ne_n}$ ,  $B_1 \cong B_{11} \otimes \cdots \otimes B_{n1}$ ,  $B_{ie_i}$  is a cyclic  $p^{e_i}$ -extension of  $B$  with a Galois group  $(\sigma_i | B_{ie_i})$ , and  $B_{i1}$  is the fixing of  $(\sigma_i^{p^1} | B_{ie_i})$  in  $B_{ie_i}$ . Clearly  $B_{1e_1} \otimes B_{21} \otimes \cdots \otimes B_{n1}$  is a cyclic  $p^{e_1}$ -extension of  $B \otimes B_{21} \otimes \cdots \otimes B_{n1}$ . Assume that  $B_{11} \otimes B_{21} \otimes \cdots \otimes B_{n1}$  has no proper idempotents. Then by Th. 1.8,  $B_{1e_1} \otimes B_{21} \otimes \cdots \otimes B_{n1}$  has no proper idempotents. By a similar method, we see that  $B_{1e_1} \otimes B_{2e_1} \otimes B_{31} \otimes \cdots \otimes B_{n1}$  has no proper idempotents. Continuing this way, it follows that  $A$  has no proper idempotents. The converse is obvious. By similar methods, we have the other assertions.

By theorems 1.3, 2.1, 2.2, and 2.3, we have the following

**Theorem 2.4.** *Let  $e_i$  ( $1 \leq i \leq n$ ) be positive integers. Then*

- (1) *there is an abelian  $(p^{e_1}, \dots, p^{e_n})$ -extension of  $B$  which has no proper idempotents if and only if there is an abelian  $(\underbrace{p, \dots, p}_n)$ -extension of  $B$  which has no proper idempotents.*

(2) *There is an abelian  $(p^{e_1}, \dots, p^{e_n})$ -extension of  $B$  which is a domain if and only if there is an abelian  $(\underbrace{p, \dots, p}_n)$ -extension which is a domain.*

(3) *There is an abelian  $(p^{e_1}, \dots, p^{e_n})$ -extension of  $B$  which is a local ring if and only if there is an abelian  $(\underbrace{p, \dots, p}_n)$ -extension which is a local ring.*

#### REFERENCES

- [ 1 ] S. U. CHASE, D. K. HARRISON and A. ROSENBERG : Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. No. **52** (1965).
- [ 2 ] G. J. JANUSZ : Separable algebras over commutative rings, Trans. Amer. Math. Soc. **122** (1966), 461—479.
- [ 3 ] K. KISHIMOTO : On abelian extensions of rings I, Math. J. of Okayama Univ., **14** (1970), 159—174.
- [ 4 ] T. NAGAHARA : On separable polynomials over a commutative ring, Math. J. of Okayama Univ., **14** (1970), 175—191.
- [ 5 ] H. TOMINAGA and T. NAGAHARA : Galois theory of simple rings, Okayama Math. Lecture, Dept. of Math., Okayama Univ., (1970).

DEPARTMENT OF MATHEMATICS  
OKAYAMA UNIVERSITY

*(Received April 1, 1971)*